The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/25/2017
01/26/2017 - UPDATED

SUBJECT:
A Vulnerability in Cisco WebEx Browser Extensions Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in the Cisco WebEx browser extension for Windows versions of Chrome, Firefox, and Internet Explorer, which could allow for arbitrary code execution. It has been confirmed by Cisco that this vulnerability does not affect Cisco WebEx browser extensions for Mac or Linux, or Cisco WebEx browser extensions for Microsoft Edge. The WebEx meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx. Successful exploitation of this vulnerability could result in the attacker gaining control of the affected system.

THREAT INTELLIGENCE:
While a proof of concept is available, there are no reports of this vulnerability being

actively exploited in the wild.

SYSTEMS AFFECTED:
- Cisco WebEx Extension for Chrome prior to 1.0.5 for Windows
- Cisco WebEx Extension for Firefox for Windows
- Cisco WebEx Extension for Internet Explorer

January 26 – UPDATED SYSTEM AFFECTED:
- ***Cisco WebEx Extension for Chrome prior to 1.0.7 for Windows***

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
A vulnerability has been discovered in the Cisco WebEx browser extensions, which could allow for arbitrary code execution. This vulnerability exists due to Cisco's WebEx browser extensions utilizing a "magic pattern" of "cwcsf-nativemsg-iframe-43c85c0d-d633-af5e-c056-32dc7efc570b.html", which can be extracted from the extensions manifest. Any website could use this magic pattern to remotely activate a visitor's Cisco WebEx browser extension, executing arbitrary code. Successful exploitation of this vulnerability could result in the attacker gaining control of the affected system.

According to the Cisco Advisory, they have begun to release software updates that address this vulnerability and that no workarounds exist to resolve the issue.

Currently, the Cisco WebEx Extension for Google Chrome version 1.0.5 contains a fix for this vulnerability. In order for Chrome users to ensure they are using the fixed version of the Cisco WebEx Extension for Google Chrome the following steps will need to be taken:

- In Chrome, open the Settings page.
- Click Extensions.
- Select the Developer mode checkbox.
- Click Update extensions now.

Internet Explorer users can take the following steps to ensure the Cisco WebEx Add-on is disabled until a patch has been released:

- In Internet Explorer, open the settings menu by clicking on the 'gear' icon.
- Click 'Manage Add-ons'
- Click on 'WebEx Productivity Tools'
- Click 'Disable'

Mozilla Firefox has disabled the Cisco WebEx Add-on and it is no longer available to download until an update has been released.

January 26 – UPDATED TECHNICAL SUMMARY:
According to the Cisco advisory, this vulnerability is due to a design defect in an application programing interface (API) response parser within the plugin. An attacker that can convince an affected user to visit an attacker-controlled web page or follow an attacker-supplied link with an affected browser could exploit the vulnerability. If successful, the attacker could execute arbitrary code with the privileges of the affected browser.

The Cisco WebEx Extension for Google Chrome version 1.0.5, which was initially released to fix this issue, did not adequately address the issue. Cisco has now released Cisco WebEx Extension for Google Chrome version 1.0.7, which does contain a fix or this vulnerability. Follow the below instructions for updating your Google Chrome extensions.

- **In Chrome, open the Settings page.**
- **Click Extensions.**
- **Select the Developer mode checkbox.**
- **Click Update extensions now.**

RECOMMENDATIONS:
The following actions should be taken:

- Install the update provided by Cisco immediately after appropriate testing.

- Users of Microsoft Windows systems can alternatively use Microsoft Edge to join and participate in WebEx session.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Cisco:
https://help.webex.com/docs/DOC-8177
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170124-webex

Chrome:
https://bugs.chromium.org/p/project-zero/issues/detail?id=1096
https://chrome.google.com/webstore/detail/cisco-webex-extension/jlhmfgmfgeifomenelglieieghnjghma

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3823